(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 197 44 786 A 1**

(51) Int. Cl.[6]: H 04 L 9/28

(21) Aktenzeichen: 197 44 786.4
(22) Anmeldetag: 10. 10. 97
(43) Offenlegungstag: 23. 7. 98

DE 197 44 786 A 1

(30) Unionspriorität:
9621274 11. 10. 96 GB

(71) Anmelder:
Certicom Corp., Mississauga, Ontario, CA

(74) Vertreter:
Flaccus, R., Dipl.-Chem. Dr.rer.nat., Pat.-Anw., 50389 Wesseling

(72) Erfinder:
Erfinder wird später genannt werden

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Digitalsignatur-Protokoll

(57) Ein Digitalsignatur-Protokoll erzeugt unter Verwendung einer Mischsumme einer verschlüsselten Nachricht einen Signaturbestandteil. Bestandteil und verschlüsselte Nachricht bilden ein Signaturpaar, das an einen Empfänger weitergeleitet wird. Beim Empfänger wird mit Hilfe der Verschlüsselungsnachricht der Verschlüsselungsschlüssel zurückgewonnen und werden die Informationen in der Nachricht beglaubigt. Das Signaturpaar kann auf einen Datenträger als Strichcode aufgetragen werden, zur Verwendung in postalischen Zustelldiensten. Durch Einsatz einer Mischsumme der Nachricht erhält man eine verringerte Nachrichtenlänge, da für die einzelnen Bestandteile der Nachricht keine individuellen Signaturen erforderlich sind.

DE 197 44 786 A 1

Beschreibung

Die vorliegende Erfindung betrifft Digitalsignatur-Protokolle. Verschlüsselungsverfahren mit öffentlichem Schlüssel sind wohlbekannt und verwenden einen öffentlichen Schlüssel und einen privaten Schlüssel, die mathematisch miteinander in Beziehung stehen. Die fehlerfesteren basieren auf der Unlösbarkeit des Problems des diskreten Logarithmus in einer endlichen Gruppe.

Bei derartigen Verschlüsselungssystemen mit öffentlichem Schlüssel werden ein Gruppenelement und ein Generator für die Gruppe eingesetzt. Der Generator ist ein Element, aus dem jedes andere Gruppenelement durch wiederholte Anwendung der zugrundeliegenden Gruppen-Operation erhalten werden kann, das heißt durch wiederholten Zusammenbau des Generators. Herkömmlicherweise wird darunter eine Potenzierung des Generators mit einem ganzzahligen Exponenten verstanden, was je nach der zugrundeliegenden Gruppenoperation als k-fache Multiplikation des Generators oder als k-fache Addition des Generators dargestellt werden kann. Bei einem derartigen Verschlüsselungssystem mit öffentlichem Schlüssel wird eine ganze Zahl k als privater Schlüssel verwendet und geheimgehalten. Ein entsprechender öffentlicher Schlüssel wird durch Potenzieren des Generators α mit der ganzen Zahl k erhalten, so daß ein öffentlicher Schlüssel in der Form α^k bereitgestellt wird. Der Wert der ganzen Zahl k kann nicht hergeleitet werden, obwohl der Exponent α^k bekannt ist.

Der öffentliche und der private Schlüssel können bei einer Nachrichtenübertragung über ein Datenkommunikationssystem eingesetzt werden, wobei einer der Teilnehmer die Daten mit dem öffentlichen Schlüssel α^k des Empfängers verschlüsseln kann. Der Empfänger empfängt die verschlüsselte Nachricht und verwendet seinen privaten Schlüssel k, um die Nachricht zu entschlüsseln und den Inhalt zurückzugewinnen. Da die ganze Zahl k nicht hergeleitet werden kann, wird beim Abhören der Nachricht der Inhalt nicht preisgegeben.

Eine ähnliche Technik kann eingesetzt werden, um die Echtheit einer Nachricht durch Verwenden einer digitalen Signatur zu verifizieren. Bei dieser Technik unterzeichnet der Sender der Nachricht die Nachricht mit einem privaten Schlüssel k, und ein Empfänger kann verifizieren, daß die Nachricht vom Sender stammt, indem er die Nachricht mit dem öffentlichen Schlüssel α^k des Senders entschlüsselt. Ein Vergleich zwischen einer Funktion der Klartextnachricht und der wiederhergestellten Nachricht bestätigt die Echtheit der Nachricht.

Zum Umsetzen eines Digitalsignatur-Verfahrens existieren verschiedene Protokolle, und einige haben große Verbreitung gefunden. Allerdings ist es bei jedem Protokoll erforderlich, einen Schutz gegen einen bedrohlichen Angriff vorzusehen, bei dem ein Betrüger möglicherweise während der Übertragung eine neue Nachricht substituiert, was den Empfänger glauben macht, daß er mit einer bestimmten Person korrespondiert. Nach der Feststellung einer derartigen Berechtigung ist es möglich, daß der Empfänger dann Informationen offenlegt, die er nicht offenlegen sollte, oder er schreibt dem Sender unrichtigerweise Informationen zu.

Um einen bedrohlichen Angriff zu vermeiden, ist es üblich, daß die Nachricht eine gewisse Redundanz enthält, zum Beispiel durch Wiederholen eines Teils der Nachricht oder in einigen Fällen der ganzen Nachricht. Dadurch wird diejenige Funktion der Nachricht gebildet, die die Echtheit bestätigt. Durch die Redundanz wird innerhalb der wiederhergestellten Nachricht ein Muster gebildet, was von dem Empfänger erwartet wird. Es ist unwahrscheinlich, daß irgendeine Manipulation an der Nachricht bei der Entschlüsselung ein derartiges Muster erzeugt, weshalb die Manipulation ohne weiteres erkannt wird.

Durch die Redundanz wird allerdings die Länge der Nachricht und somit die zum Übertragen der Nachricht erforderliche Bandbreite vergrößert. Im allgemeinen ist dies unerwünscht, und die Auswirkung davon ist als reduzierte Übertragungsrate für die Nachricht zu sehen. Bei einigen Anwendungen allerdings ist die Länge der Nachricht kritisch, da die unterzeichnete Nachricht möglicherweise als gedrucktes Dokument reproduziert wird und die Länge der Nachricht dann den Umfang des gedruckten Dokuments beeinflußt. Eine derartige Anwendung besteht in einem postalischen Umfeld, wo ein Strichcode eingesetzt werden kann, um Ziel, Postgebühr, Rate und den Sender anzuzeigen. Um Betrug zu vermeiden, wird die Nachricht von einer Berechtigungsstelle digital unterzeichnet, und ein digitaler Strichcode wird zusammengestellt, der die in der unterzeichneten Nachricht enthaltenen Informationen darstellt. Was die Lesbarkeit und das Verhindern von Fehlern, die beispielsweise durch das Auslaufen von Farbe hervorgerufen werden, betrifft, so unterliegt die Strichcodedarstellung bestimmten physikalischen Begrenzungen. Eine lange Nachricht erzeugt infolgedessen einen übermäßig langen Strichcode, insbesondere dann, wenn die zum Verhindern des bedrohlichen Angriffs erforderliche Redundanz durch die Wiederholung der gesamten Nachricht gebildet wird.

Die Länge der Nachricht ist besonders bei digitalen Unterschriften von Nachrichten akut, die aus diskreten Blöcken zusammengebaut sind, wie beispielsweise in einem derartigen postalischen Umfeld. Bei einem herkömmlichen Signaturprotokoll wird ein kurzfristiger Geheimschlüssel k (der Sitzungsschlüssel) gewählt und zum Potenzieren des Generators α der zugrundeliegenden Gruppe verwendet, um einen kurzfristigen öffentlichen Schlüssel $r=\alpha^k$ zu erhalten. Von r wird eine Bitkette r' hergeleitet und zum Verschlüsseln der Nachricht in verwendet, um Schlüsseltext e zu erhalten, das heißt $e=E_{r'}(m)$, wobei $E_{r'}$ die Anwendung eines Verschlüsselungs-Algorithmus mit dem Schlüssel r' auf die Nachricht (m) bezeichnet.

Es wird ein Signaturbestandteil s erzeugt, der Informationen enthält, damit die Echtheit der Signatur verifiziert werden kann. Die Natur des Signaturbestandteils hängt von dem umgesetzten Protokoll ab, doch kommt bei einem typischen beispielhaften Protokoll ein Signaturbestandteil s der Form $s=ae+k \bmod(n)$ zum Einsatz, wobei n die Ordnung der Gruppe ist. Die Werte des Signaturpaars s, e werden weitergeleitet.

Bei diesem Protokoll berechnet der Empfänger $\alpha^s(\alpha^{-a})^e$, wobei α^{-a} der öffentliche Schlüssel des Senders ist, um α^k zu erhalten, das den kurzfristigen öffentlichen Schlüssel r darstellt.

Zum Zurückgewinnen der Nachricht m kann der Schlüsseltext e dann unter Verwendung des Schlüssels r' entschlüsselt werden.

Wenn eine Nachricht aus mehreren Blöcken zusammengesetzt ist, d. h. $m=m_1; m_2; m_3$, kann der Schlüsseltext e für den Block m_1 erhalten und das entsprechende Paar s, e weitergeleitet werden. Allerdings hängt der Signaturbestandteil s von der Verschlüsselung des ersten Blocks ab, was die nachfolgenden Blöcke anfällig macht. Es ist deshalb erforderlich, jeden Block zu unterzeichnen und mehrfache Signaturen weiterzuleiten, die alle die Länge der Nachricht vergrößern.

Eine Aufgabe der vorliegenden Erfindung besteht somit darin, die obigen Nachteile zu vermeiden oder zu lindern.

Allgemein ausgedrückt, erzeugt die vorliegende Erfindung eine verschlüsselte Nachrichtenkette e mit einem Schlüssel r', und der Schlüsseltext wird an den Empfänger

weitergeleitet. Die verschlüsselte Nachrichtenkette e wird auch durch eine Hash-Funktion verarbeitet, und die resultierende Mischsumme e' wird in der Signatur s verwendet. Der Empfänger stellt die Nachricht wieder her, indem er die Nachrichtenkette e einem Hashing unterzieht und mit Hilfe des Wertes den Verschlüsselungsschlüssel r' wiederherstellt. Die Nachricht kann dann aus der Nachrichtenkette e wieder hergestellt werden.

Die Redundanz kann gegebenenfalls überprüft werden, um die Genauigkeit der Nachricht sicherzustellen, es muß aber nur ein Signaturpaar übertragen werden. Da die Signatur aus der Mischsumme der verschlüsselten Nachrichtenkette e erzeugt wird, können einzelne Datenblöcke nicht verändert werden.

Als weitere Präferenz kann das die Nachricht begleitende Zertifikat als einer der Blöcke in die Nachricht eingebaut und signiert werden. Das Zertifikat weist die erforderliche Redundanz für die Berechtigung auf, weil aber die Mischsumme der Kette in der Signatur verwendet wird, erfordert die Symmetrie der Blöcke keinerlei Redundanz. Dementsprechend kann eine kürzere Nachricht verwendet werden.

Ausführungsformen der Erfindung werden nunmehr unter Bezugnahme auf die beiliegenden Zeichnungen lediglich beispielhaft beschrieben. Es zeigen:

Fig. 1 eine schematische Darstellung eines Datenkommunikationssystems;

Fig. 2 eine schematische Darstellung eines Blocks von Nachrichten;

Fig. 3 ein Flußdiagramm, das das Erzeugen einer digitalen Signatur und das Wiederherstellen einer Nachricht zeigt; und

Fig. 4 eine der **Fig.** 2 ähnliche schematische Darstellung einer alternativen Ausführungsform.

Unter Bezugnahme auf **Fig.** 1 enthält ein Datenkommunikationssystem **10** ein Teilnehmerpaar **12, 14** und einen Kommunikationskanal **16**. Wie durch die durchgezogene Linie angezeigt, kann der Kommunikationskanal **16** ein unterbrechungsfreier Kanal zwischen den beiden Teilnehmern **12, 14** sein, so daß zwischen den Teilnehmern digitale Informationen übertragen werden können. Es versteht sich allerdings, daß der Kanal **16**, wie durch strichpunktierte Linien angedeutet, unterbrochen sein kann, so daß der Sender **12** mit einer Strichcode-Zusammenstelleinrichtung **18**, die digitale Informationen empfängt, in Verbindung steht, sie in einen Strichcode umwandelt und Strichcodeangaben **20** auf einen Umschlag **22** druckt. Die Angaben **20** können dann mit einem Strichcodelesegerät **24** gelesen und die wiederhergestellte Nachricht an den Empfänger **14** übermittelt werden.

Jeder der Teilnehmer **12, 14** enthält eine Verschlüsselungseinheit **26** bzw. **28**, die digitale Informationen verarbeiten und sie zur Übertragung durch den Kanal **16** vorbereiten kann, wie unten beschrieben wird.

Wie in **Fig.** 2 zu erkennen ist, beabsichtigt der Teilnehmer **12**, eine digitale Botschaft m zu erzeugen, die verschlüsselt und über die Strichcodezusammenstelleinrichtung auf den Umschlag **22** aufgebracht werden kann. Die digitale Nachricht m besteht aus mehreren diskreten Blöcken m_1, m_2, m_3, . . ., die jeweils ein bestimmtes Teil der Informationen darstellen. Bei der Nachricht m_1 kann es sich beispielsweise um die Adresse des Senders handeln, die Nachricht m_2 kann die Adresse des Empfängers sein, die Nachricht m_3 kann die zutreffende Postgebühr sein, und die Nachricht m_4 kann die berechnete Postgebühr sein und ein elektronisches Abbuchen bewirken.

Um die Nachricht m digital zu unterzeichnen, läßt der Teilnehmer **12** sie durch die Verschlüsselungseinheit **26** verarbeiten. Die Einheit **26** enthält einen Zahlengenerator **30**, der eine zufallsmäßige ganze Zahl k wählt und bei einer Potenziereinheit **32** einen kurzfristigen öffentlichen Schlüssel r berechnet. Die Einheit **26** kann unter jedem der bewährten Verschlüsselungsverfahren laufen, eine besonders günstige Realisierung jedoch verwendet elliptische Kurven über einem endlichen Feld. Der kurzfristige öffentliche Schlüssel r wird von dem Generator der Gruppe α hergeleitet, die mit der ganzen Zahl k potenziert wird, so daß $r=\alpha^k$ ist. Bei einer Umsetzung mit einer elliptischen Kurve ist die zugrundeliegende Feldoperation die Addition, so daß die "Potenzierung" durch k-fache Addition eines Punktes P erhalten wird, so daß der öffentliche Schlüssel ein Punkt kP auf der Kurve ist.

Eine Bitkette r' wird aus r erhalten, indem ein vorbestimmter Algorithmus, wie beispielsweise eine modulo-Reduktion, oder, wenn die Umsetzung über eine elliptische Kurve geschieht, eine Koordinate des den öffentlichen Schlüssel darstellenden Punktes angewendet wird, und von der Verschlüsselungseinheit als Schlüssel zum Verschlüsseln jedes der Blöcke m_1, m_2 usw. beim Verschlüsselungsmodul **34** verwendet. Die verschlüsselten Blöcke e; e_2; . . ., werden zu einer Nachrichtenkette e verkettet, wobei $e=e_1//e_2// \ldots, e_k$ und wobei allgemein $e_i=E_r(m_i)$ in einem Register **36** ist.

Die Verschlüsselungseinheit **26** beinhaltet eine bei **38** angedeutete Hash-Funktion, die die Schlüsseltextkette e so verarbeitet, daß eine verkürzte Bitkette entsteht, die die Mischsumme e' umfaßt. Geeignete Hash-Funktionen sind sichere kryptographische Einweg-Hash-Funktionen wie zum Beispiel SHA.

Von einer Arithmetikeinheit **40** wird dann unter Verwendung der Mischsumme e' und des privaten Schlüssels k, von dem der Verschlüsselungsschlüssel r abgeleitet ist, ein Signaturbestandteil s erzeugt. Ein geeigneter Bestandteil weist die Form

$$s = ae' + k \bmod(n)$$

auf, wobei a der langfristige Privatschlüssel des Teilnehmers **12** und k der vom Teilnehmer **12** gewählte kurzfristige private Schlüssel ist.

Die Verschlüsselungseinheit stellt die Nachricht zusammen und sendet die Nachrichtenkette e und den Signaturbestandteil s als Signaturpaar von einem Sender **42** durch den Kanal **16**. Bei Einsatz als postalisches System kann die Nachricht dann in einen wahrnehmbaren Code, wie zum Beispiel einen zweidimensionalen Strichcode, übersetzt werden, als Angaben **20** auf einen Datenträger **22** aufgetragen werden, wie in **Fig.** 1 angedeutet, und später von dem Empfänger **14** gelesen werden. Je nach der jeweiligen Anwendung ist es möglich, daß die Angaben **20** sichtbar wahrgenommen werden, wie bei einem gedruckten Strichcode, magnetisch durch Drucken mit magnetischer Farbe, oder sie könnten von einem Laser optisch gelesen werden.

Bei Empfang durch den Empfänger **14** am Empfangsgerät **50** berechnet die Verschlüsselungseinheit **28** anfänglich den Hash-Wert e'*, indem die empfangene Nachrichtenkette e mit der Hash-Funktion h, wie bei **52** angedeutet, einem Hashing unterzogen wird. Ein öffentlicher Schlüssel r*, der mit der ganzen Zahl k in Beziehung steht, wird dann in der Arithmetikeinheit **54** berechnet, wobei Operationen in dem zugrundeliegenden Feld verwendet werden, um den Generator α mit dem empfangenen Wert des Bestandteils s zu potenzieren, und der öffentliche Schlüssel des Teilnehmers **12** mit dem berechneten Hash-Wert e'* potenziert wird, das heißt

$$r^* = \alpha^s(\alpha^{-a})^{e'^*}.$$

Aus dem wiederhergestellten öffentlichen Schlüssel wird dann ein Verschlüsselungsschlüssel r*' hergeleitet.

Ein Verschlüsselungsmodul **56** verarbeitet dann die empfangene Nachrichtenkette e, wobei der Verschlüsselungsschlüssel r*' verwendet wird, um die Nachricht in wiederherzustellen. Die Nachricht m enthält die erforderliche Redundanz, die überprüft werden kann, um die Echtheit der Nachricht festzustellen.

Es versteht sich, daß die in **Fig. 3** umrissene Prozedur als Software realisiert und auf einem Allzweckrechner ausgeführt oder in einer integrierten Spezialschaltung realisiert werden kann.

Man wird bemerken, daß der Hash-Wert e' eine Mischsumme aller verschlüsselten Blöcke ist, die verkettet sind, weshalb es nicht möglich ist, einen der Blöcke zu manipulieren, ohne den resultierenden Hash-Wert zu beeinflussen. Obwohl mehrere Blöcke gesendet und wiederhergestellt werden, ist nur eine Signatur erforderlich, was die Nachrichtenlänge insgesamt reduziert.

Eine weitere Ausführungsform ist in **Fig. 4** gezeigt, bei der gleiche Bezugszeichen gleiche Parameter bezeichnen, wobei der Übersichtlichkeit halber die Nachsilbe "a" angefügt ist.

Bei der Ausführungsform von **Fig. 4** beinhaltet die Nachricht m als Nachrichtenblock m_{5a} ein von einer sicheren Berechtigungsstelle ausgestelltes Zertifikat. Das Zertifikat enthält ausreichend Informationen, um die Authentifizierung des öffentlichen Schlüssels des Teilnehmers **12** und der Parameter des zugrundeliegenden Systems zu gestatten. Die Nachrichtenkette e wird wie oben angedeutet zusammengestellt, indem jeder der Blöcke verschlüsselt wird, um eine Kette e_{1a}, e_{2a} usw. einschließlich dem Zertifikat m_{5a} zu liefern.

Es wird dann die Mischsumme e'_a erhalten, die verwendet wird, um einen Signaturbestandteil s_a der Form

$$s_a = ae'_a + k \bmod(n)$$

zu erzeugen.

Nach Wiederherstellung durch den Empfänger **14** enthält die wiederhergestellte Nachricht das Zertifikat m_{5a}, das als Teil der zugrundeliegenden Systemparameter die erforderliche Redundanz aufweist. Durch die Redundanz des Zertifikates m_{5a} wird somit die Nachricht m beglaubigt und die Notwendigkeit der Redundanz in den weiteren Blöcken vermieden. Da die in der Signatur s verwendete Mischsumme eine Mischsumme aller Blöcke ist, ist es jedoch nicht möglich, einen Block innerhalb der Nachricht zu ersetzen **5** und gleichzeitig die Echtheit der Signatur zu bewahren.

Es versteht sich, daß der Signaturbestandteil s jede beliebige geeignete Form aufweisen kann, die gewöhnlich in Digitalsignatur-Protokollen verwendet wird, die die Wiederherstellung des kurzfristigen öffentlichen Schlüssels und somit des Verschlüsselungsschlüssels aus einer Mischsumme der verschlüsselten Nachricht gestatten.

Patentansprüche

1. Digitalsignatur-Protokoll zum Beglaubigen digitaler Informationen, die von einem Teilnehmer über ein Datenkommunikationssystem zu einem anderen übertragen werden, wobei das Protokoll folgende Schritte umfaßt: Erzeugen eines öffentlichen Schlüssels aus einer ganzen Zahl k, Verschlüsseln einer die Informationen enthaltenden Nachricht mit einem aus dem öffentlichen Schlüssel hergeleiteten Verschlüsselungsschlüssel, um einen Schlüsseltext e der Nachricht zu bilden, Anwenden einer Hash-Funktion auf den Schlüsseltext, um eine Mischsumme e' zu bilden, Erzeugen eines die Mischsumme e' und die ganze Zahl k beinhaltenden Signaturbestandteils s, Weiterleiten eines den Schlüsseltext e und den Bestandteil s enthaltenden Signaturpaars an den anderen Teilnehmer, Unterziehen des von dem anderen Teilnehmer empfangenen Schlüsseltextes e einem Hashing mit der Hash-Funktion, um eine empfangene Mischsumme e'* zu erhalten, Verwenden der empfangenen Mischsumme e'*, um aus dem Signaturbestandteil den Verschlüsselungsschlüssel wiederherzustellen, und Zurückgewinnen der Nachricht in aus dem Schlüsseltext e durch Anwenden des wiederhergestellten Schlüssels r.

2. Digitalsignatur-Protokoll nach Anspruch 1, bei dem der Schlüsseltext als wahrnehmbarer Code auf einen Datenträger zur Übertragung von einem Teilnehmer zum anderen aufgetragen wird.

3. Digitalsignatur-Protokoll nach Anspruch 2, bei dem der Code ein zweidimensionaler Strichcode ist.

4. Digitalsignatur-Protokoll nach Anspruch 1, bei dem der Signaturbestandteil einen zweiten privaten Schlüssel des einen Teilnehmers enthält und bei der Wiederherstellung des Verschlüsselungsschlüssels ein dem zweiten privaten Schlüssel entsprechender öffentlicher Schlüssel verwendet wird.

5. Digitalsignatur-Protokoll nach Anspruch 4, bei dem die Nachricht ein Zertifikat zum Beglaubigen des dem zweiten privaten Schlüssel entsprechenden öffentlichen Schlüssels enthält.

6. Digitalsignatur-Protokoll nach Anspruch 4, bei dem der Signaturbestandteil s die Form
$s = ae' + k$ aufweist, wobei
a der zweite private Schlüssel,
e' die Mischsumme des Schlüsseltextes e und
k die ganze Zahl ist.

7. Digitalsignatur-Protokoll nach Anspruch 1, bei dem die Nachricht aus mehreren diskreten Nachrichten zusammengestellt ist, von denen jede verschlüsselt und übersetzt wird, um den Schlüsseltext zu bilden.

8. Digitalsignatur-Protokoll nach Anspruch 1, bei dem der öffentliche Schlüssel von einem Punkt auf einer elliptischen Kurve hergeleitet wird.

9. Vorrichtung zum Erzeugen einer digitalen Signatur einer Nachricht m zur Übertragung über ein Datenkommunikationssystem, wobei die Vorrichtung folgendes umfaßt: einen Potenzierer zum Erzeugen eines öffentlichen Schlüssels r aus einem privaten Schlüssel k, ein Verschlüsselungsmodul zum Verschlüsseln der Nachricht m mit einem aus dem öffentlichen Schlüssel r hergeleiteten Schlüssel und Erzeugen eines Schlüsseltextes e, eine Hash-Funktion zum Durchführen von Operationen an dem Schlüsseltext e und Erzeugen einer Mischsumme e' des Schlüsseltextes, eine Arithmetikeinheit zum Erzeugen eines die Mischsumme e' und den privaten Schlüssel k beinhaltenden Signaturbestandteils und ein Sendegerät zum Senden eines den Signaturbestandteil und den Schlüsseltext umfassenden Signaturpaars über das Kommunikationssystem.

10. Vorrichtung nach Anspruch 9, wobei die Arithmetikeinheit einen Signaturbestandteil der Form
$s = ae' + k$ erzeugt, wobei
a ein zweiter privater Schlüssel,
e' die Mischsumme des Schlüsseltextes e und
k der private Schlüssel ist.

11. Vorrichtung nach Anspruch 9 mit einem Strichcodegenerator zum Erzeugen eines wahrnehmbaren Strichcodes des Signaturpaars auf einem Träger.

12. Vorrichtung zum Verifizieren einer über ein Daten-

kommunikationssystem empfangenen digitalen Signatur, wobei die Vorrichtung folgendes enthält: ein Empfangsgerät zum Empfangen eines Signaturpaars mit einem einen privaten Schlüssel k und eine Mischsumme e' von Schlüsseltext e einer Nachricht in und den Schlüsseltext e beinhaltenden Signaturbestandteil s, eine Hash-Funktion zum Durchführen von Operationen an dem Schlüsseltext e und Liefern einer Mischsumme e'*, eine Arithmetikeinheit zum Wiederherstellen eines mit dem privaten Schlüssel k in Beziehung stehenden öffentlichen Schlüssels und ein Verschlüsselungsmodul zum Anwenden eines von dem öffentlichen Schlüssel hergeleiteten Verschlüsselungsschlüssels auf den Schlüsseltext und Wiederherstellen der Nachricht m.

13. Vorrichtung nach Anspruch 12, bei der der Signaturbestandteil die Form
$s = ae' + k$ aufweist, wobei
a ein zweiter privater Schlüssel,
e' eine Mischsumme des Schlüsseltextes e und
k der private Schlüssel ist.

14. Vorrichtung nach Anspruch 12 mit einem Strichcodelesegerät zum Lesen eines das Signaturpaar darstellenden Strichcodes auf einem Träger.

Hierzu 3 Seite(n) Zeichnungen

Numm
Int. Cl.[6]:
Offenlegungstag:

DE 197 44 786 A1
H 04 L 9/28
23. Juli 1998

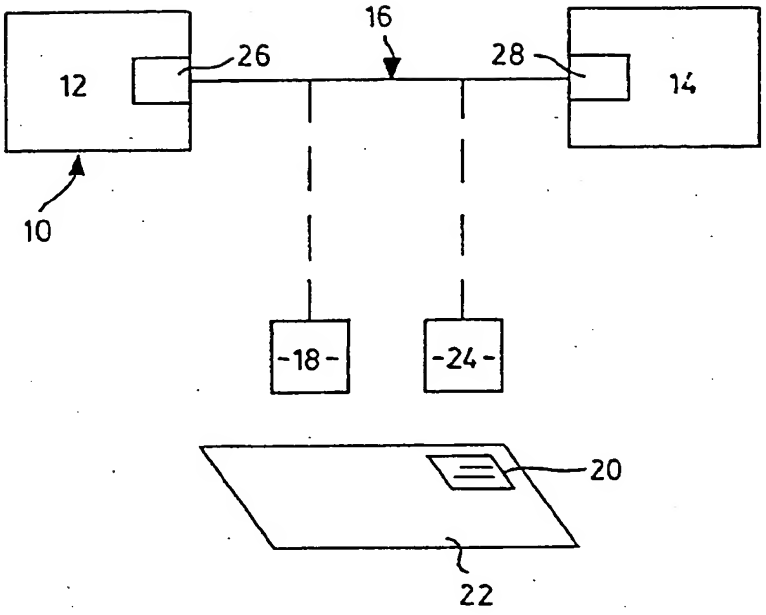

FIG. 1

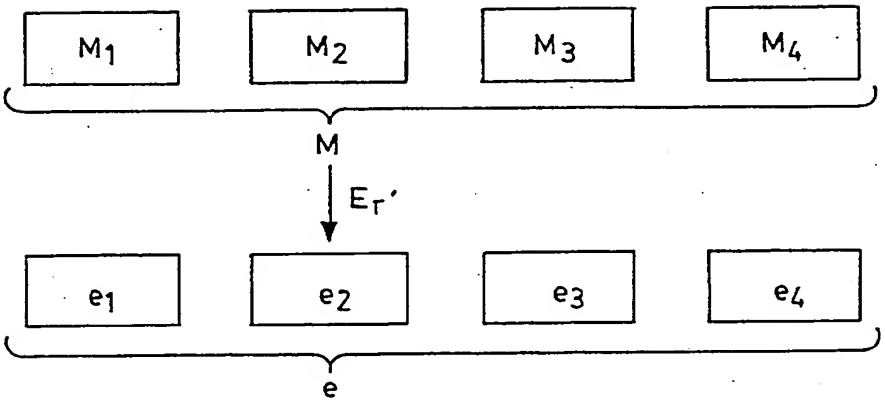

FIG. 2

Nu[redacted]:
Int. Cl.[6]:
Offenlegungstag:

DE 197 44 786 A1
H 04 L 9/28
23. Juli 1998

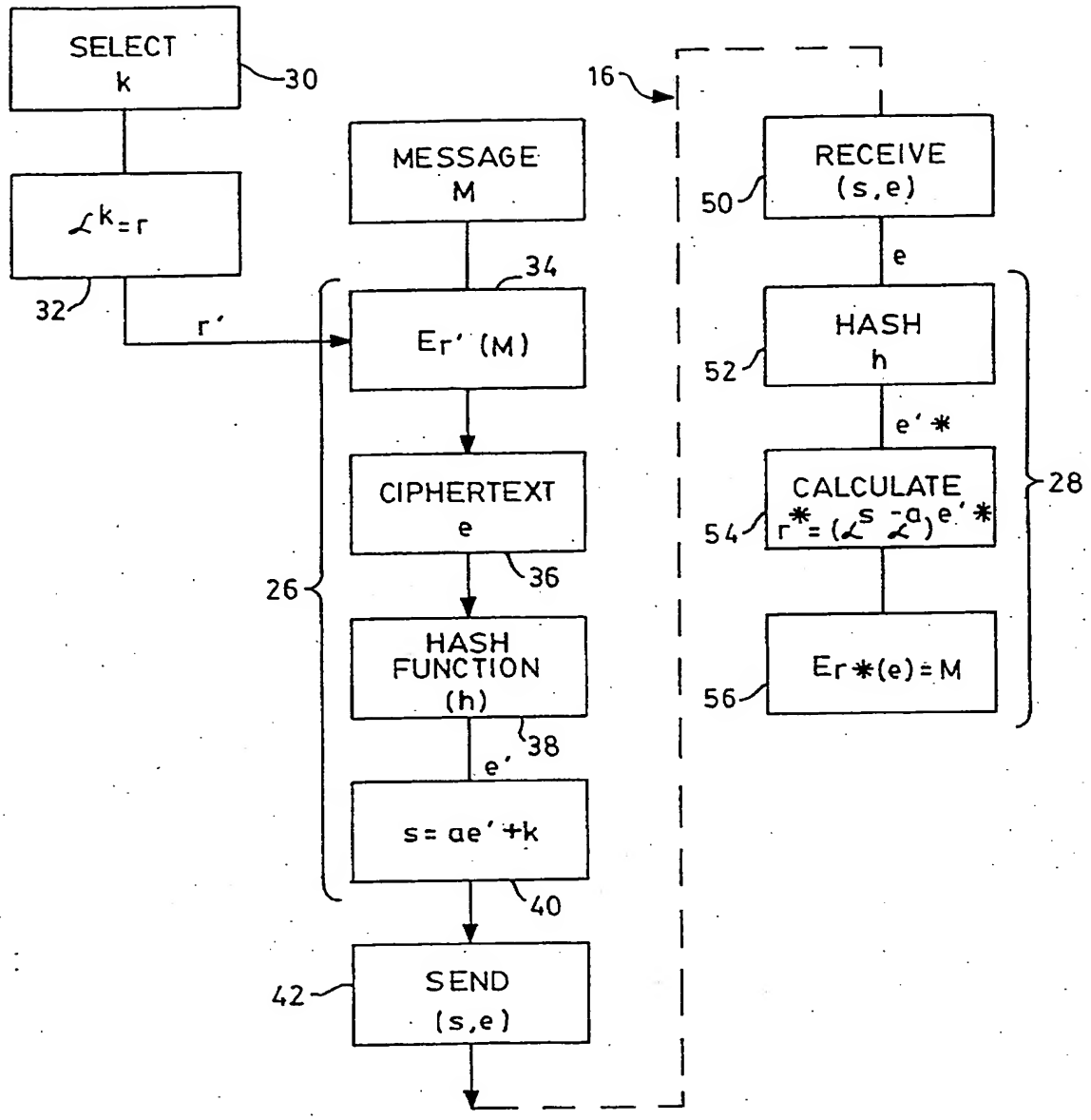

FIG. 3

Numm
Int. Cl.[6]:
Offenlegungstag:
DE 197 44 786 A1
H 04 L 9/28
23. Juli 1998

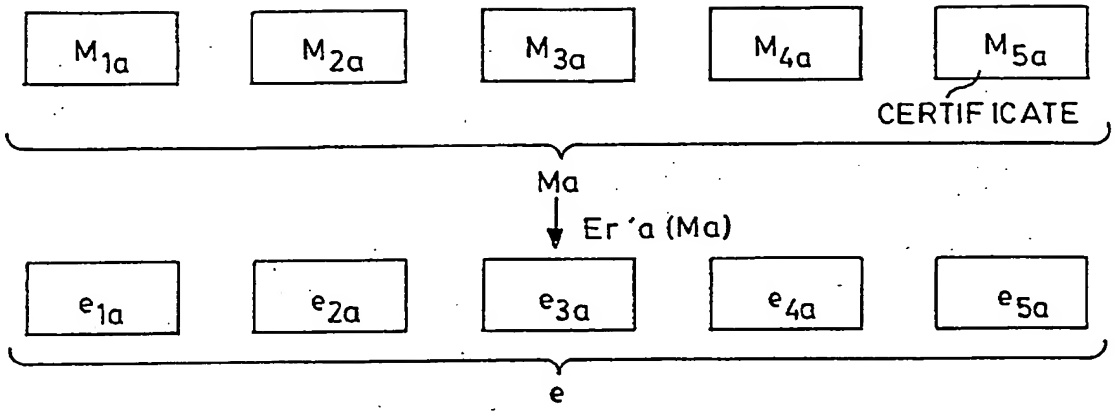

FIG. 4